THIS PAGE BLANK (USPTO)

PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	WO 99/17537
H04N 1/32	A1	(43) International Publication Date:	8 April 1999 (08.04.99)

(21) International Application Number: PCT/US98/20196

(22) International Filing Date: 24 September 1998 (24.09.98)

(30) Priority Data:
08/939,215   29 September 1997 (29.09.97)   US

(71) Applicant *(for all designated States except US)*: HEWLETT–PACKARD COMPANY [US/US]; 3000 Hanover Street, M/S 20BN, Palo Alto, CA 94304 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: NATARAJAN, Balas, K. [–/US]; 18079 Reed Knoll Road, Los Gatos, CA 95030 (US).

(74) Agent: YIP, Philip, S.; Hewlett–Packard Company, Legal Dept., 20BN, 3000 Hanover Street, Palo Alto, CA 94304 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: WATERMARKING OF DIGITAL OBJECT
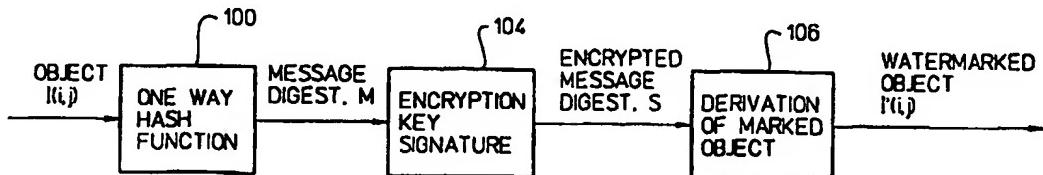
(57) Abstract

A technique for identifying digital object using a digital watermark. The technique includes the steps of encrypting a message derived from source data on the digital object, to obtain an encrypted message digest (S); deriving a watermark from the encrypted message digest (S); and incorporating the watermark into the source data. The encryption is preferably done with a public key encryption system. The message to be encrypted can be obtained via performing a hash function on the source data on the digital object to obtain a message digest (M). The message digest (M) is the message encrypted with the signature encryption key to obtain the encrypted message digest (S). The watermark is resistant to cropping, scaling, and truncation.

WATERMARKING OF DIGITAL OBJECT

FIELD OF THE INVENTION

5

The present invention is related to techniques for watermarking digital data, and more specifically, to watermarking digital data such as images and audio data for authenticating copyright ownership.

10
BACKGROUND

Because of the rapid increase of electronic commerce in the recent years, secured data transaction is becoming more and more important. To prevent electronic data to be appropriated by unauthorized parties, cryptographic methods

15 have been used to transmit digital data between consenting parties to guard against unintended exposure to other parties. Various kinds of data, including military information, financial transaction, personal data, and the like can be transmitted via cryptography to protect the data.

In the arena of protecting the right to original art or literary works, in the past,
20 most violations were by unauthorized parties making physical copies of authorized copies of the original (e.g., copyrighted) works. Copies of physical artistic material, such as copyrighted paintings, photographs, phonographs, and analog audio tapes, are usually perceptibly inferior to the originals. The degradation of fidelity in the

1

copying process, e.g., in photocopying or photography, is a factor in deterring

unauthorized copying of such material. Today, many visual, audio, literary, or other

proprietary works are stored and transmitted digitally. Such digital material can be

copied over and over without significant loss in fidelity. The risk to the owner of an

5   original artistic work, or proprietary work, is that once the digital data are transmitted,

if data suspected to be copies of the transmitted data are found, the verification of

whether the suspect data are copied from the originally transmitted data, for example,

digital data of a piece of art work, is usually impossible.

        Recently, digital watermarking has been devised as a security technique to

10   facilitate the identification of the source of digital material for the purpose of, for

example, copyright enforcement. The watermark is an identification code that is

imbedded in the original digital data and is preferably imperceptible to the human

observer of the artistic work. One example of a scheme for watermarking involves

inserting an identification string into a digital audio signal to substitute the

15   insignificant bits of randomly selected audio samples with the bits of an identification

code. Another example of watermarking relating to watermarking video digital

works involves assigning a predetermined value to a predetermined coding parameter

that, when modified, requires a plurality of further parameters to be modified in order

to correctly decode the video signal. In one watermarking technique each copy of an

20   object is marked with an identifier code. More recently, a watermarking scheme in

which a two-dimensional spread spectrum signal is added to an image has been

proposed. To verify the watermark in a given image, the original image is subtracted

2

from the given image and the correlation of the difference image to the watermark signal is computed.

Although much advance has been made in watermarking digital data, generally, prior techniques of watermarking suffer from a variety of shortcomings. Often, the original image is necessary to verify the presence of the watermark. Manipulative operations such as cropping to cut out a portion of the work and scaling to obtain a work of larger or smaller size pose a considerable problem on the verification process. Many times the watermarking scheme is invertible, i.e., an attacker (or temperer), based on a first watermarked image but without knowledge of what the first watermark is, would be able to compute a second image and a second watermark such that inserting the second watermark into the second image would result in the first watermarked image. Such invertible watermarking schemes can make the verification of authentic copies of a copyrighted work difficult. Further, it may even lead to ownership disputes on valuable digital data since an unscrupulous person might appropriate another's watermarked material, subtract from it his own watermark and claim the resulting product to be his own. Often, in prior watermarking techniques, changes in contrast or brightness may fool the verification algorithms, making them less reliable. Furthermore, many of the watermark schemes do not offer a mechanism for creating and managing watermarks. This means that if the same watermark is used to protect several works, compromise in the secrecy of the watermark will compromise the protection for all of the works. What is needed a watermarking technique that can these deficiencies. The present invention provides a watermarking technique that is resistant to cropping, invertible, resistant to brightness

or contrast changes, and will not compromise other related watermarked works if the mechanism of watermarking in one watermarked work is disclosed.

SUMMARY

5   The present invention provides a technique for identifying digital object using a digital watermark. This technique can be easily implemented using computers. The technique includes encrypting data derived from a set of source data on the digital object, deriving from the encrypted data a watermark, and incorporating the watermark into the source data. Preferably, the source data of the digital object are

10   processed through a hash function to obtain a message digest (M) on the digital object and the message digest (M) is encrypted with a signature encryption key to obtain an encrypted message digest (S). Further, the encryption of the message digest (M) is preferably done with a public key-private key encryption system. Because the preferred mode is to process the source data through a one-way hash function to

15   obtain a message digest, for clarity and convenience, the set of data for encryption derived from the set of source data is termed a "message" or "message digest" herein although they do not necessarily have to have been through a one-way hash function. The set of encrypted data is called "encrypted message digest" herein for the same reason.

20   The present watermarking technique is versatile and can be advantageously employed to watermark a variety of digital objects, including audio, video, image, multimedia data, and the like. Further, the present technique offers high security because it is not easily foiled by attackers. For example, by a using a hash function in

4

conjunction with encryption in which a private key is kept confidential, the present technique offers the advantage of being not invertibility, unlike many prior watermarking techniques. Therefore, it is very difficult for an attacker to backcompute the original watermark by the disclosure of immediate information. To further increase security, in an embodiment of the present invention a public key encryption system is employed. As a result, a suspect object (i.e., an object suspected to be copied from an original, e.g., copyrighted, object) can be checked with the public key of the original object's owner to determine whether the watermark is present without compromising the other watermarked objects. In the embodiment in which an encryption technique involving a public key is used, ownership of an object can be established to a neutral party, such as a court of law, using only the public key of the object's owner, without requiring the owner to reveal his private key. Also, the watermark is not removed by lossy compression (in which less perceptually important information is severed to reduce the size of the data file) or cropping (in which a portion of the object is cut). In the embodiment in which the watermarking vector is orthogonal to the vector of the pixels into which the watermark is to be inserted, changes in the brightness or contrast will not fool the verification algorithm.

BRIEF DESCRIPTION OF THE DRAWINGS

The following figures are included to better illustrate the embodiments of the technique of the present invention. In these figures, like numerals represent like features in the several views.

Figure 1 is a block diagram showing an embodiment of the watermarking technique of the present invention.

Figure 2 is a block diagram showing in further detail an embodiment of the watermarking technique of Fig. 1

5   Figure 3 shows a flow diagram of an embodiment of a watermarked object being obtained from a digital object according to the present invention.

Figure 4 shows how a suspect object is evaluated to determine whether it is derived from a watermarked object, according to an embodiment technique of the present invention.

10   Figure 5 shows a picture printed from a digital image.

Figure 6 shows a picture printed from a digital image having a watermark incorporated into the digital image of Fig. 5.

Fig. 7 shows a correlation spread of Fig. 6.

Fig. 8 shows a cropped and JPEG- compressed watermarked image of Fig. 5,

15   showing the resistance to distortion by compression and cropping.

Fig. 9 shows a correlation spread of Fig. 8, showing the sensitivity of the evaluation for the presence of watermark in the object even when the object has been cropped and compressed.

Fig. 10 shows a truncated watermarked image of Fig. 5, showing the resistance

20   to distortion by truncation.

Fig. 11 shows a correlation spread of Fig. 10, showing the sensitivity of the evaluation for the presence of watermark in the object even when the object has been truncated. '

6

DETAILED DESCRIPTION

The present invention provides a technique for inserting a digital watermark in to a digital object and for evaluating a digital object for the watermark. An encryption technique is used in the derivation of the watermark and the watermark is incorporated into the digital object in such a way to render it extremely hard for an attacker (i.e., one who tampers with the watermarked data to remove or change the watermark) to derive the original digital object from the watermarked digital object. The digital watermark is resistant to cropping, scaling, inadvertent distortions, as well as the intentional removal or corruption of the watermark by an attacker.

A digital object that can be watermarked with the technique of the present invention is referred to as a "physical object" in that it can be an digital visual image; digital audio program, e.g., music; digital tactile data, e.g., data which can be transformed into tactile information that can be sensed by touch; multimedia data; or simply digital data strings that can be divided into discrete segments arrangeable into rows and columns of "pixels." One obvious example of such pixels would be, for an image, the pixels of digital information obtained by scanning a color photograph into digital information representing rows and columns of color dots (commonly known in visual display technology as "pixels"). Thus, a digitized photograph may contain hundreds of rows and columns of pixels. However, in this disclosure, "pixels" can be the discrete segments of digital data for other types of digital information, e.g., those mentioned in the above. In the case of sound recording, for example, a sound signal

may be sampled by an A/D converter, which would output samples having values representative of the characteristics of the sound signal at particular time segments. The technique for obtaining pixels of data on visual images, audio signals, and other data streams are well known in the art. Any conventional technique for obtaining the

5 digital objects is applicable. As another example, a digital camera or a computer running a computer graphics software can be used to generate digital images directly. Similarly, music can be converted from sound waves to digital data by using A/D converters. These digital objects, as well as other types of digital objects, are applicable in the present invention.

10 An embodiment of the watermarking technique of the present invention is depicted in Fig. 1. A digital object, $I(i,j)$, having m rows and n columns of pixels, is processed through a hash function 100 (e.g., a one-way hash function such as the MD5 function) to result in a message digest M. The function of the hash function is to take the input data $I(i,j)$ and convert them into a fixed-size string (hash), and

15 preferably a much shorter string for a large object, much as a fingerprint, of the input data $I(i,j)$. Preferably, the hash is generated in such a way that it is very difficult to generate the original input data from the hash, i.e., the message digest M. This difficulty of back calculation is beneficial because if an attacker were able to derive the input data from the hash, he might be able to remove or change the watermark.

20 Many hash functions are known in the art and can be applied in the present technique. One applicable one-way hash function (or message digest algorithm) known in the art is the MD5 method. Other examples of applicable one-way hash functions include the SNEFRU function, SHA function, and HAVAL function. (See Schneier, B.,

8

Applied Cryptography, John Wiley and Sons, 1993, pp. 333-346 for a discussion on one-way hash functions.) A person skilled in the art will know how to apply such hash functions to a digital object. In general, in selecting a hash function H(F) that operates on an arbitrary-length message F to obtain a fixed-length hash value, h,

5

$$h = H(M),$$

the following characteristics are desired: Given M, it is easy to compute h; given h, it is hard to compute M; and given M, it is hard to find another message M' with the

10   property H(M) = H(M'). Preferably, the hash function is selected such that it is resistant to brute force attacks, as well as Birthday attacks, which are based on the occurrence of two random messages that return the same value through the same hash function.

The message digest M is then encrypted with a signature. The encryption

15   algorithm can either be a public key-private key system (asymmetric data encryption algorithm) or a private key system (symmetric data encryption algorithm). Such an encryption imparts a unique feature in the message digest M that will distinguish these encrypted data from other data, thus acting much like a physical signature on a physical document. If a private key alone is used for encryption, this private key

20   preserves the secrecy of the original message and encrypted message digest is invertible, i.e., an attacker cannot back calculate the message digest M or the original object from the encrypted message digest. However, if it is necessary to prove ownership, e.g., to a third party such as a court of law, to verify the owner's

9

signature, the owner would have to reveal his private key. With the private key

revealed, his other watermarked objects that are marked with the same or similar

private key watermark might be compromised since an attacker might be able to gain

access to his private key to use it to obtain information on the watermarking of the

5   other objects.

A more preferable way would be to use a public key-private key encryption

system (referred to as the "public key system" hereinafter unless specified otherwise).

In encryption using the public key system, the user possess a matched pair of keys: a

private key and a public key. The private key is kept secret and is known only to the

10   user whereas the public key can be distributed widely. A message encrypted with

either key can only be decrypted with the other key. If a user encrypts a message

with his private key, then the message can only be decrypted with his public key.

Because only the user has the private key, the encrypted message can be decrypted

only with his public key. Since the private key is known only to the encryptor, it is

15   established that if the encrypted message can be decrypted with the user's public key,

he must have encrypted the message, i.e., he has "signed" the message with his

"signature." The strength of the signature is dependent on knowing that the public

key of the user is genuine. For this reason, public keys are preferably notarized or

certified by third parties. In this invention, when the public key system is used, the

20   private key is used to encrypted the message to create the watermark from the

original image. When it is necessary to prove ownership of a watermark, the public

key can be provided, e.g., to a verifying third party, to verify the owner's signature.

The advantage of using public key encryption in this invention is that since the

private key is used to produce the watermark from the original object, it will be impossible, or extremely difficult, for an attacker to remove the watermark from the watermarked object to create a false original without the private key, even if he had access to the public key.

5   In either the private key system case or the public key system case, the private key of the encryption algorithm is necessary to back-calculate from the encrypted M to obtain the original M. Many encryption algorithms are known in the art and can be used for this purpose. A good example is RSA algorithm. Other applicable public key encryption algorithms include ELGAMAL algorithm and DSS (digital signature

10   standard) algorithm. Many other encryption algorithms are also known in the art, e.g., POHLIG-HELLMAN algorithm, RABIN algorithm, and DES (data encryption standard) algorithm, see Schneier, B., *Applied Cryptography, supra*. A person skilled in the art will know how to apply such encryption algorithms to a digital object.

15   It is noted that the encryption step, either using a public key system or a private key system, can be used to encrypt the digital object directly without processing through a hash function, as long as the private key is kept secret. However, if the digital image is large, extremely long computational time will be needed. The hash function reduces the size of the data that requires encryption to

20   produce the watermark.

After the encrypted message digest S is formed, it is processed (block 106) to derive the watermarked object I'(i,j). In an embodiment, shown in Fig. 2, to derive the watermarked object I'(i,j), the encrypted message digest S is modulated, e.g., to

modify the amplitude of the signal, to spread over a perceptually significant region of the spectrum (block 108). By this process (block 108), a key vector V, representing a physical domain signal, is obtained. Spreading the message digest S over a large part of the spectrum has the advantage of rendering the watermark substantially

5   imperceptible to the human sense organ for which the object is designed. Further, the watermark will be preserved if the data is manipulated by processes such as compression or cropping. For example, spreading the message digest S over a substantial part of the spectrum would not overly distort a certain small range of colors in a visual image or distort a certain small range of audio frequency. Since a

10   useful watermark preferably is preserved when undergoing lossy compression or cropping, the watermark is placed in the portion of the spectrum in the perceptually significant portion of the spectral frequencies. If such a watermarked object is cropped to remove the watermark (e.g., by an attacker), the object would be distorted sufficiently that its quality would be substantially inferior to the original object or the

15   watermarked object. A person skilled in the art will know what portion of the spectrum to modulate for a particular object without undue experimentation.

From the key vector V, a watermark vector W applicable for inserting into a selected portion of the original object I(i,j) is obtained (block 110). As will be described later, the watermark vector W is dependent on the particular portion of the

20   original object I(i,j) selected for the insertion of the watermark. After incorporating the watermark into the original object I(i,j) by combining the watermark vector V with the selected portion of the original object I(i,j), the watermarked object I'(i,j) is obtained (block 112).

12

To better illustrate the preferred embodiment of the invention, an example of watermarking a visual image is provided below. It is to be understood that other types of physical objects, for example, those mentioned above, e.g., audio digital objects, tactile digital object, and the like, can be similarly watermarked by a person skilled in the art based on the present disclosure.

Example

The process is described in general and illustrated in Fig. 3 as follows

(1) A digital object image $I(i,j)$ with m rows and n column of pixels is obtained. A message digest of the data bits in $I(i,j)$ is computed, using a standard message algorithm such as the MD5 function, to obtain the message digest M.

(2) The message digest is signed to create the owner's signature, with encryption methods such as the RSA method or Elliptic Curve, thus obtaining the encrypted message digest S.

(3) Let S be the bits of the signature for constructing a watermark. For example, S may have 512 bits. A vector U of n entries is constructed, where n corresponds to the number of columns of pixels. Alternately, the vector can have m entries corresponding to the number of rows, m. If that is the case, the following steps referring to rows will be applied to columns instead, and vice versa. In constructing U in this example, the second bit to the 65th bits are assigned a modulation value depending on whether the corresponding bits (e.g., the first 64) of the encrypted message digest S are 0 or 1. The rest of the bits in encrypted message digest S are assigned values of 0. The first bit of S is assigned a value of 0 to

13

correspond to the DC component of the pixels. For example, in the second to the 65th bits of U, a bit is assigned a value of -1 for a corresponding bit of 0 in S; the bit in U is assigned a 1 for a corresponding bit of 1 in S. It is to be understood that the modulation can have other optional values, as long as they are consistent and the resulting watermark would not overly distort the object. For example, a bit in U, instead of having a value of -1, may be assigned a value of 2; and a bit of 1 in U, may be assigned a value of -1. Furthermore, the first bits of U may have more bits or less bits than 64. However, a longer U would require more computer power to implement the watermark, and a smaller U is more prompt to be broken by an attacker. The first bits of U correspond to the lower frequencies, which are the more conceptually significant frequencies of the visual image object. This is also true for audio digital works. However, it is conceivable that in other works where the perceptually significant bits are in the higher frequencies, the higher frequency bits of U will be modulated. Furthermore, the first bits of U need not be based on the first bits of S, but optionally can be based on some other bits as long as they are consistent. For example, the first bits of U can be based on the last bits, the middle bits, or alternate bits, or the like of S. The first bit in S (corresponding to the DC component) having a value of 0 makes the watermark resistant to changes in brightness or contrast.

(4) A reverse Fourier transform of U is performed to obtain a key vector V. It is to be understood that other types of transforms, e.g., reverse Discrete Cosine Transform (DCT), can be used to transform U from the frequency domain to a physical domain, e.g. time domain (for example, for audio and other time variant signals) or spatial domain (for, example, for images, video, or other spatially varying

14

signals). A person skilled in the art will know how to select and apply such
transforms to obtain the key vector V based on the present disclosure to derive a
watermark.

(5) A portion of the original object I(i,j) is selected, e.g., b contiguous rows,
and this portion is averaged to construct a reference vector A relating to the image
pixels for orthogonalization calculation. In this example, the reference vector A is an
average vector calculated by averaging data. Depending on the object, one may want
to select the whole object, or a portion thereof that has conceptually important details.
For example, b can be 16 in the middle section of the image, indicating that 16 rows
in the middle section is to be averaged to form A. Then, to reduce the risk that the
key vector V would have a dependency on the vector A, i.e., would depend on the
columnic position of the elements in the b rows of the object, preferably the key
vector V is orthogonalized with respect to the reference vector A, thereby obtain a
watermark vector W. The orthogonalization can be represented by the equation:

$$W = V - (\hat{V} \cdot \hat{A}) A \qquad \text{Eq. 1}$$

$$\text{where } \hat{V} = \frac{V}{\sqrt{V \bullet V}}$$

$$\text{and } \hat{A} = \frac{A}{\sqrt{A \bullet A}}$$

15

$\hat{A}$ is the unit vector along A. The watermark vector W represents the frequency and magnitude data of the digital watermark that is to be incorporated into the original object I(i,j).

(6) The watermark vector W is incorporated into the original object I(i,j), preferably, by inserting into the portion of the I(i,j) from which the reference vector A has been derived. A common method of inserting the watermark vector W is by adding a small scaled version of W back to each of the b rows selected for the reference vector A earlier. This method of obtaining the watermarked elements I'(i,j) in the object can be represented by the following equation:

$$I'(i,j) = I(i,j) + a(i,j) \, W(i,j) \qquad \text{Eq. 2}$$

In Eq. 2 a is a proportional constant, which may vary depending on the positions of i or j if preferred.

In a preferred embodiment,

$$I(i,j) = c \cos (2\pi i / b) \qquad \text{Eq. 3.}$$

Typically, c is chosen such that the watermark signal is roughly – 40dB PSNR (peak signal to noise ratio). Other methods of inserting watermarks can also be used. For example, multiple scaling factors a that depend on other factors can be used. Additional watermarks can be added to other locations of the digital object as desired,

16

by repeating the orthogonalization and the watermarking steps using the same key vector V. Alternative methods of incorporating watermark using watermark factors are apparent to one skilled in the art based on the present disclosure (see, e.g., Cox, et al. *supra*, which is incorporated by reference herein). In the example shown in Fig. 3, the b rows of the original digital object are replaced with the b rows of watermarked pixels. Thus the watermarked object $I'(i,j)$ (which has the same number of rows m and the same number of columns, n, as the original object) includes b rows of watermarked elements, whereas the remaining (m-b) rows of elements remain unchanged from the same rows in the original digital object. The resulting watermark is a one-dimensional watermark in that it involves all the columns in the variation of i or j in Eqs. 2 to 3, or other similar equations. This one-dimensional watermark is mathematically simpler than a two dimensional watermark in which the W varies as a function of the rows as well as the columns. However, if desired, a two-dimensional watermark can be created such that a watermark matrix W_m having elements that are derived from the process of one-way hash function and encryption. For example, W_m can be derived from V by incorporating V with various proportional constants into the elements at various columns and rows in W_m. This foregoing description is just one example, a skilled person will know how to derive a two-dimensional watermark from the present disclosure.

Given a suspect image $I''(i,j)$ suspected of being derived (e.g., copied) from the watermarked object $I'(i,j)$, the suspect image can be evaluated by the following method, which is illustrated in Fig. 4. This method requires the watermark vector V and the average row vector A. In this method, each block of b contiguous rows in

17

the suspect image for the watermark is successively evaluated. For example, the first b contiguous rows can be evaluated, then the b contiguous rows starting from the second row to the (1+b)th row, then the third row to the (2+b)th row, and so on.

(A) In each block to be evaluated, the b rows are averaged to obtain a reference vector A".

(B) The vector A" is orthogonalized with respect to A to obtain a suspect watermark vector X. The mathematics of orthogonalizing A" is similar to that of orthogonalizing the key vector V in Eq. 1.

(C) The relative closeness of X to W is computed, e.g., by calculating the correlation between the W and X. The equation for calculating the correlation between X and W a is as follows:

$$ \text{Correlation} = \frac{W \cdot X}{\sqrt{(W \cdot W)(X \cdot X)}} \qquad \text{Eq. 4} $$

(D) Step (C) is repeated to compute the relative closeness of X to W for all the blocks of contiguous b rows. The maximum of the relative closeness over all the blocks of b rows is then taken. If this relative closeness is above a predetermined threshold value, then the suspect image is deemed to contain the watermark.

(E) If the suspect image $I''(i,j)$ is cropped or scaled, a horizontal search by searching at various match locations along the reference vector A'' can be performed to get the best relative closeness, i.e., to arrive at the maximum correlation of the watermark to the suspect object. Further, a search can be conducted for reflections of the digital object about the axes.

(F) Synthesize a number of random candidate watermark vectors (e.g., one hundred watermarks) with the same spectral properties as V. Compute the correlation of each of these candidate vectors with the suspect digital object $I''(i,j)$, at the location, scale, and crop factors at which the correlation of W was maximized.

(G) Compare the correlation obtained from the original watermark against the correlation obtained for the random vectors. If the former and the latter are far apart, then it is likely that the suspect object $I''(i,j)$ contains the watermark key vector V. In other words, it is likely that suspect object $I''(i,j)$ has the watermark of the original object $I(i,j)$, and therefore is likely to have been derived from it.

The above deals with detecting whether a suspect object is derived from an original object. In the case that the ownership of a digital object $J(i,j)$, e.g., a digital image, is in dispute, the ownership can be established via determining the presence of a watermark by a neutral third party such as a judge. A person claiming ownership of the digital object will present to the judge his original image $I(i,j)$ corresponding to $J(i,j)$ and the signature S of the hash of that original digital object, and his public key for decryption. He would further declare the location in the digital object $J(i,j)$ where the watermark can be found and the scaling and cropping factors of $J(i,j)$ with respect to his original object $I(i,j)$. The judge can verify using the following process.

19

(A) Compute a message digest of the bits in I(i,j). Decrypt S with the public key presented by the claimant. The bit strings for the message digest computed and the decrypted S should be the same if the claimant is the owner of J(i,j). Otherwise, reject the claimant's claim of ownership.

5   (B) Construct the watermark vector V from the signature S. At the specified location of the object J(i,j) compute the correlation of the watermark vector V after compensating for cropping and scaling. Use the original object I(i,j) to compute the corresponding reference vector A.

(C) Synthesize random candidate watermarks with the same spectral properties

10   of V. Compute the correlation of each of these candidate vectors with the object J(i,j) and compare the correlation obtained with V to the correlation obtained with the random candidate vectors as in the aforementioned method for dectecting the presence of a watermark in a suspect digital object. If the two correlation types are far apart, then it is likely the object J(i,j) contains the watermark vector V, i.e., contains the watermark

15   of the object I(i,j) provided by the claimant.

In this example a digital image was evaluated. The original image object used in this illustrative example is shown in the picture of Fig. 5. The original image object has 256 (m rows) x 384 (n columns) of pixels. The watermarked image is shown in Fig. 6. The strength of the watermark is ~45DBPSNR. A comparison of Fig. 5 and Fig. 6 shows

20   that there is no perceptual difference that is distinguishable to the human eye. What can be distinguished by the human sense organs, e.g., the eye, has been known in the art or can be determined without undue experimentation. Fig. 7 shows the correlation spread obtained by a verification algorithm for the watermarked image of Fig. 6 using the above

correlation method. In Fig. 7, the abscissa shows the various spurious watermarks with the same spectral properties as the true watermark embedded in the image. The spurious watermarks were synthesized by the verification algorithm. The spike "sp" in the middle of the figure corresponds to the correlation when applied to the image with the true watermark, whereas the rest of the graph shows the correlation when applied to randomly generated watermarks and the true watermark of the same spectral bandwidth.

To evaluate the robustness of the watermark in its resistance to distortion by cropping and compression, the digital object of Fig. 5 was cropped to 176 X 274 pixels and JPEG_compressed with substantial loss, achieving a compression ration of 28.6 (JPEG is a standard lossy compression method, see Bhaskaran and Konstantinides, *Image and Video compression standards*, Kluwer Publishers). The cropped, compressed image was decompressed to result in the image of Fig. 8. Fig. 9 shows the correlation spread for the image of Fig. 8. A tall spike "spc" is clearly seen in the middle of the spread, indicating the presence of the watermark, thus identifying that the picture of Fig. 9 as being derived from the image of Fig. 5. Similarly, making a downscaled version of the image of Fig. 5 and computing the correlation spread of the downscaled image (not shown in the figures) indicate that the watermarking was verifiable after downscaling, thus showing that the watermark is resistant to scaling. Further, Fig. 10 shows the picture of the image of Fig. 5 after truncation with setting to zero the five least significan bits of each eight-bit pixel in the watermarked image of Fig. 6. Fig. 11 shows the correlation spread obtained by processing through the detection procedure for the image of Fig. 10. Again, a clear spike "spt" is seen in the correlation spread. Thus, this evaluation on truncation shows that the watermark is resistant to truncation.

21

The technique of watermarking a digital object and evaluating a suspect digital object for the presence of the watermark according to the present invention can be implemented with digital electronics that are capable of data manipulation and calculation based on the equations described herein above. Such applicable digital electronics include microprocessors and computers, e.g., personal computers, minicomputers, and mainframe computers. Furthermore, the algorithms for the data manipulation and calculation can be stored in digital storage devices, such as compact discs, floppy discs, hard discs, magnetic tapes, and the like, which can then be loaded or read into the microprocessors or computers for implementation of the watermarking and evacuation processes. Such digital storage devices are generally articles of manufacture having a suitable digital storage medium readable by the microprocessors or computers. It is also contemplated that various computers can be networked so that digital objects can be transferred between computers to be watermarked and evaluated for watermarks. It is also to be understood that the various steps in the watermarking process described above can be done separately by different computers and processors and the results be combined to achieve the overall function of watermarking or evaluation for the presence of watermark, as well as both.

Although the preferred embodiment of the present invention has been described and illustrated in detail, it is to be understood that a person skilled in the art can make modifications within the scope of the invention.

WHAT IS CLAIMED IS:

1.   A method for identifying digital object using digital watermark, comprising:

(a) encrypting a message derived from source data on the digital object to obtain an encrypted message digest (S); and

(b) deriving a watermark from the encrypted message digest (S) and incorporating into the source data.

2.   A method according to claim 1 wherein the message is obtained via performing a hash function on the source data on the digital object to obtain a message digest (M) on the digital object, and wherein the message digest (M) is the message encrypted with the signature encryption key to obtain the encrypted message digest (S).

3.   A method according to claim 1 wherein the watermark is a physical domain watermark and the method further comprises incorporating the physical domain watermark to at least a portion of the source data.

4.   A method according to claim 3 further comprising transforming a frequency domain vector (U) derived from the encrypted message digest (S) to physical domain in deriving the watermark.

5.   A method according to claim 4 further comprising deriving the frequency domain vector (U) by modulating at least a portion of the encrypted message digest (S) to obtain at least a portion of the vector (U).

6.   A method according to claim 5 wherein a portion of the vector (U) corresponds to low frequencies and another portion of (U) corresponds to high frequencies, the portion of U corresponding to low frequencies being derived by modulating at least a portion of the encrypted message digest (S).

7.   A method according to claim 6 wherein the portion of the vector (U) corresponding to low frequencies are modulated to have more significant impact on amplitude of the watermark than the portion of the vector (U) corresponding to high frequencies.

8.   A method according to claim 7 wherein the portion of the vector (U) corresponding to low frequency has negative value in elements corresponding to "0" bits of the at least a portion of the encrypted message digest (S) and has positive value in elements corresponding to "1" bits of the at least a portion of the encrypted message digest (S); and wherein the portion of (U) corresponding to high frequencies have elements of zero value.

9.   A method according to claim 1 wherein the source data consist of rows and columns of pixels and the watermark is represented by a watermark vector (W)

having a dimension corresponding to the number of rows (m) or the number of columns (n) of the pixels.

10.   A method according to claim 9 wherein a pixel contains data on a discrete section of an image object.

11.   A method according to claim 9 wherein a pixel contains data on a discrete section of audio object.

12.   A method according to claim 9 wherein the watermark incorporated into the source data is orthogonal to the data to which the watermark is added.

13.   A method according to claim 9 further comprising deriving from the source data a source data vector (A) having the same dimension as that of the watermark vector (W) by selecting at least a portion of the source data and further comprising deriving the watermark vector (W) based on the encrypted message digest (S) such that watermark vector (W) is orthogonal to source data vector (A); and further comprising combining the watermark vector (W) with the data in the selected portion of the source data from which source data vector (A) is derived to form watermarked data.

14.   A method according to claim 9 further comprising comparing the at least a portion of the source data before incorporation of the watermark to after incorporation of the watermark.

25

15.　　　　　A method according to claim 14 further comprising finding the correlation between the watermark vector (W) and a target vector (X) derived from data suspected of containing the watermark, wherein said target vector (X) is orthogonal to the source data to which the watermark is incorporated.

16.　　　　　A method for identifying data using digital watermark, comprising:

(a) performing a one-way function on source data to obtain a message digest (M);

(b) encrypting the message digest (M) with a signature encryption key to obtain an encrypted message digest (S);

(c) deriving a frequency domain vector (U) from the encrypted message digest (S) by modulating a portion of the encrypted message digest (S) corresponding to low frequencies more than a portion corresponding to high frequencies;

(d) transforming the frequency domain vector (U) into a physical domain key vector (V);

(e) selecting a portion of the source data and deriving a watermarking vector (W) from the frequency domain vector (U) orthogonal to the selected source data; and

(f) combining the selected source data with the watermarking vector (W) in the physical domain.

17.'　　　　A system for identifying data using digital watermark, comprising:

26

(a) means for encrypting a message derived from source data with a signature encryption key to obtain an encrypted message digest (S); and

(b) means for deriving a watermark from the encrypted message digest (S) and incorporating into the source data.

18.   A system according to claim 17 further comprising a means for performing a hash function on the source data to obtain a message digest (M) and wherein the means for encrypting encrypts the message digest (M) with the signature encryption key to obtain the encrypted message digest (S).

19.   A system according to claim 17 wherein the water mark is a physical domain watermark and the means for deriving incorporates the physical domain watermark to at least a portion of the source data.

20.   A system according to claim 19 wherein the means for deriving derives a frequency domain vector (U) from the encrypted message digest (S) and transforms the vector (U) to physical domain in deriving the watermark.

21.   A system according to claim 20 wherein the means for deriving derives the frequency domain vector (U) by modulating at least a portion of the encrypted message digest (S) to obtain at least a portion of the vector (U).

27

22.   A system according to claim 21 wherein the means for deriving manages the source data as rows and columns of pixels and derives a watermark vector (W) based on the vector (U), the watermark vector (W) having a dimension corresponding to the number of rows (m) or the number of columns (n) of the pixels.

23.   A system according to claim 22 wherein the means for deriving derives from the source data a source data vector (A) having the same dimension as that of the watermark vector (W) by selecting at least a portion of the source data and wherein the watermark vector (W) is orthogonal to source data vector (A).

24.   A system according to claim 23 further comprising a means for comparing a set of target data with the source data, the means for comparing compares a target vector (X) derived from the target data to the source data, the target vector (X) being orthogonal to the source data vector (A).

25.   An article of manufacture comprising a program storage medium, tangibly embodying a program code means readable by a computer to cause the computer to identifying a digital object using a digital watermark, comprising:

(a) code means for performing a one-way function on source data on the digital object to obtain a message digest (M) on the source data;

(b) code means for encrypting the message digest (M) with a signature encryption key to obtain an encrypted message digest (S);

28

(c) code means for deriving a watermark from the encrypted message digest (S) via a transforming a portion of the message digest (S) as frequency domain into a physical domain before resulting in a one-dimensional watermark for incorporating into the source data; and

(d) code means for incorporating the one dimensional watermark into the source data.

OBJECT
I(i,j) → [ONE WAY HASH FUNCTION] 100 → MESSAGE DIGEST, M → [ENCRYPTION KEY SIGNATURE] 104 → ENCRYPTED MESSAGE DIGEST, S → [DERIVATION OF MARKED OBJECT] 106 → WATERMARKED OBJECT I'(i,j)

Fig. 1

ENCRYPTED MESSAGE DIGEST, S → [MODULATION OVER SPECTRUM] 108 → KEY VECTOR, V → [DERIVATION OF WATERMARK] 110 ← OBJECT, I(i,j) OR PORTION → WATERMARK W → [INCORPORATION OF WATERMARK] ← 'OBJECT, I(i,j) → WATERMARKED OBJECT
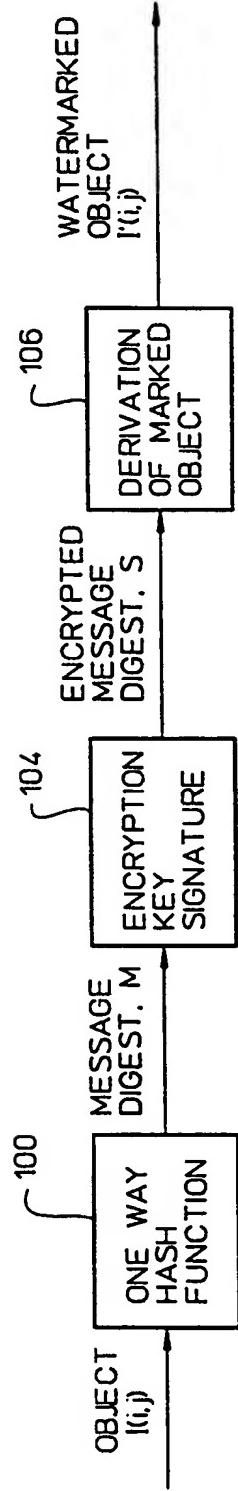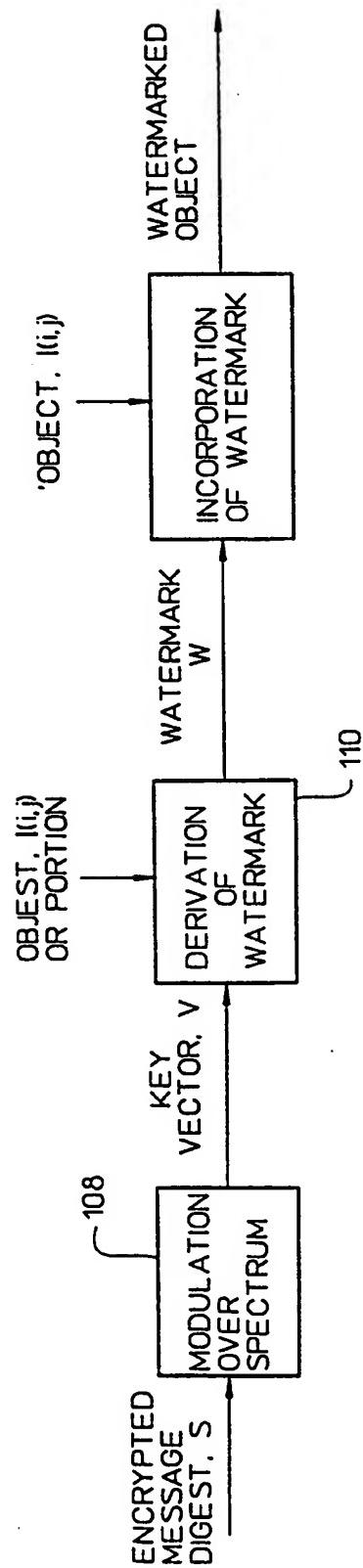
Fig. 2
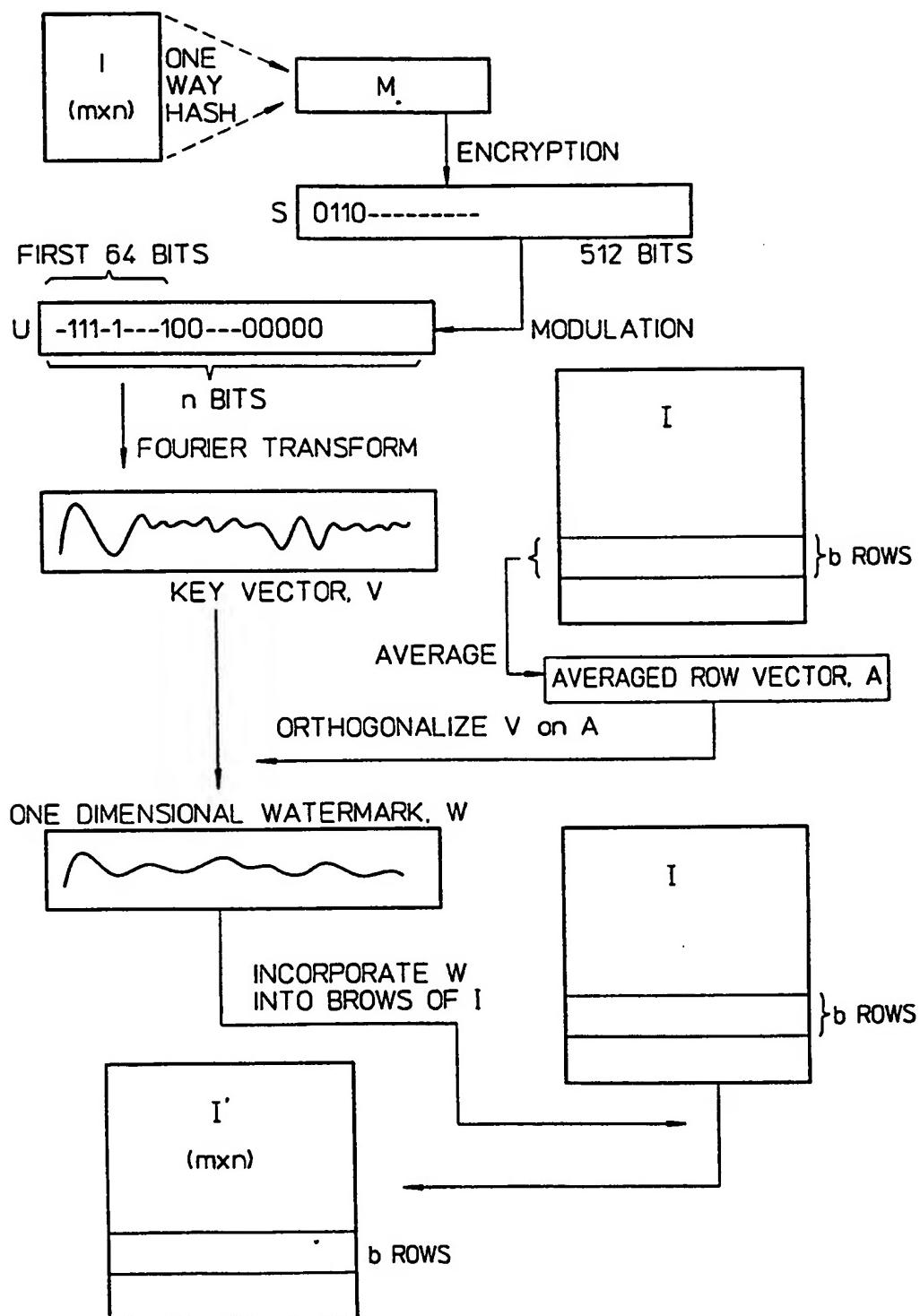
Fig. 3
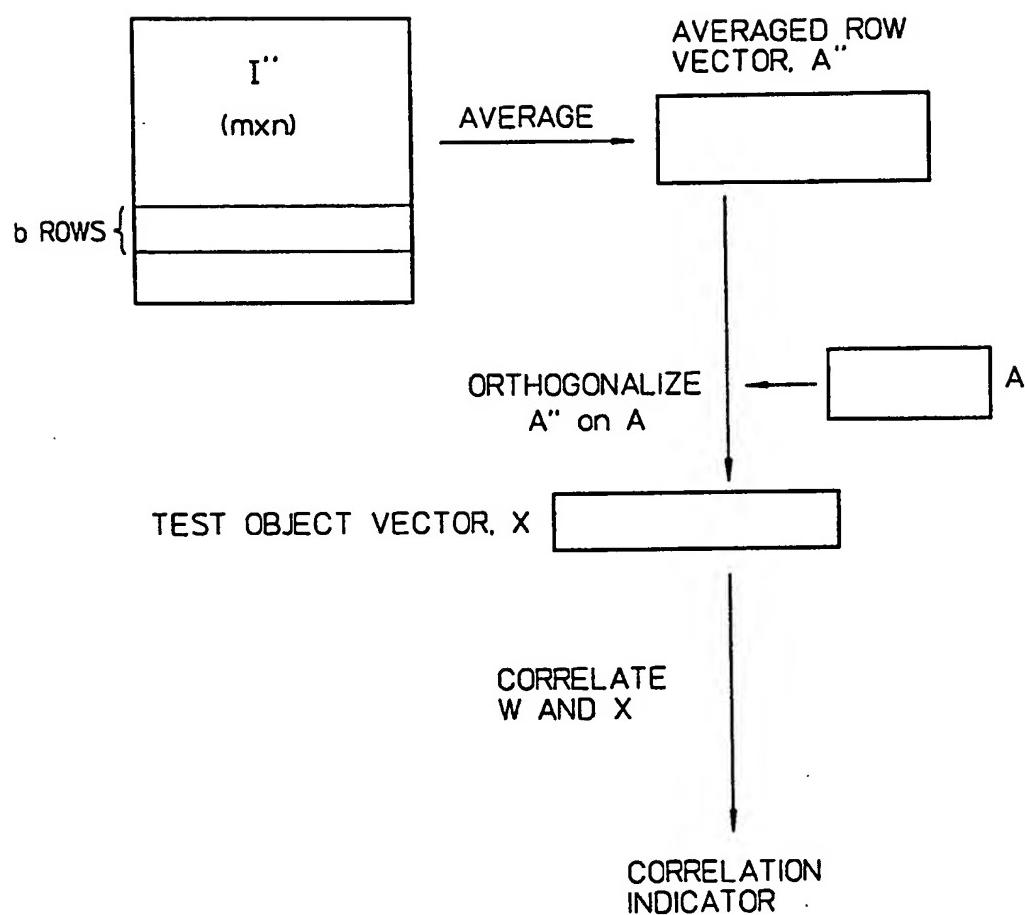
Fig. 4
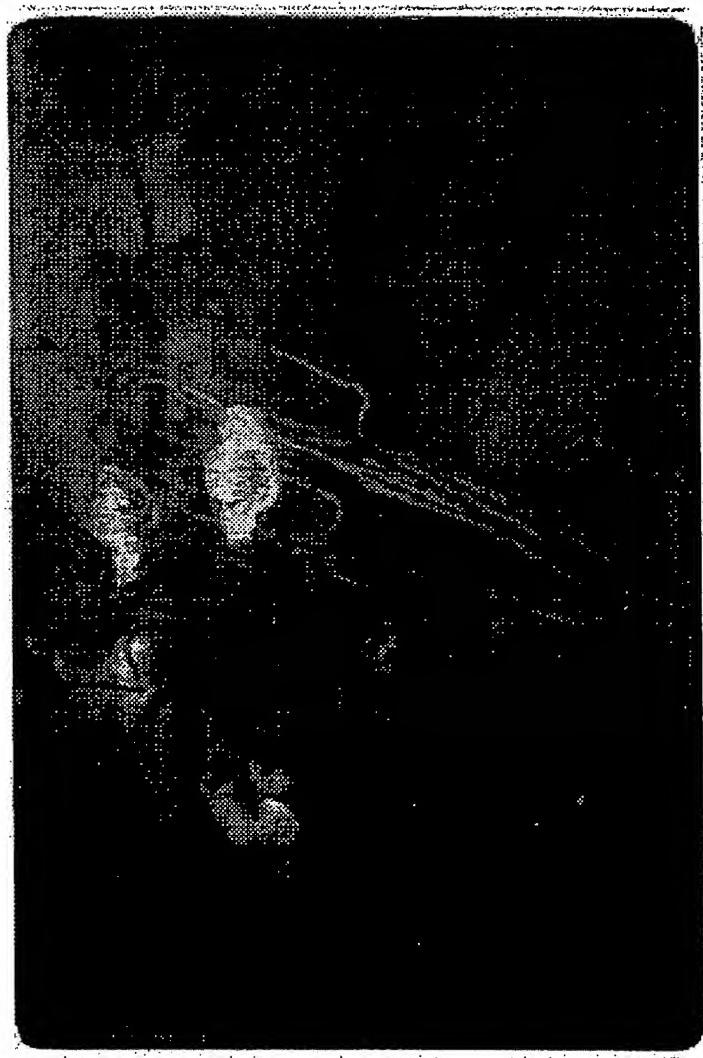
Fig. 5
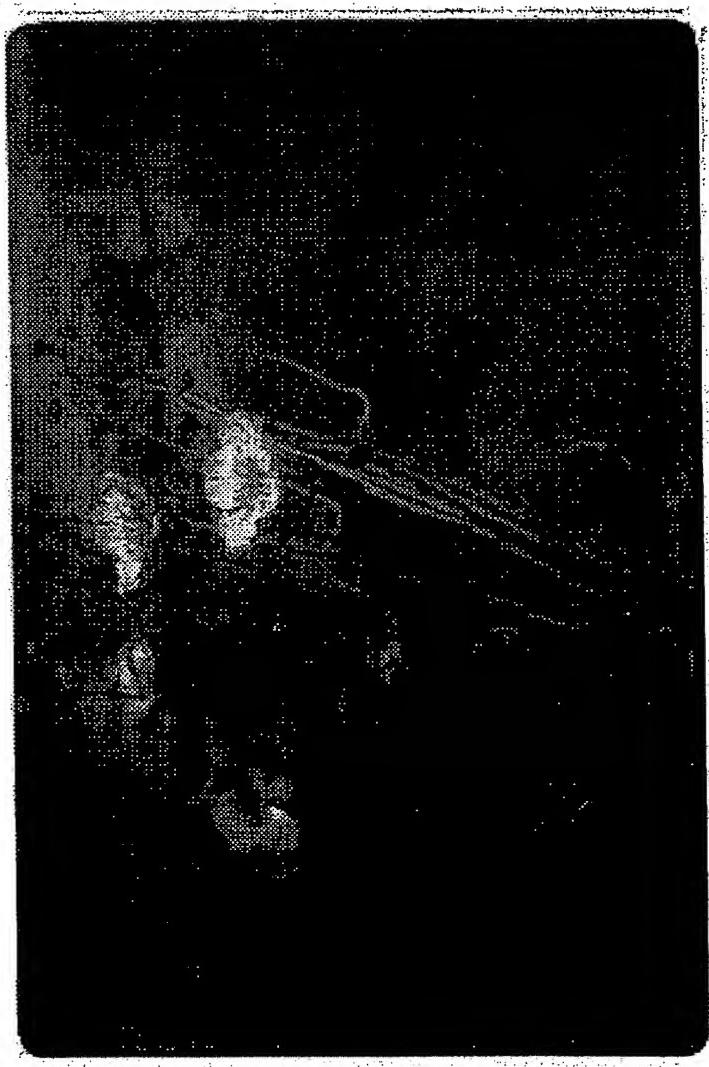
Fig. 6
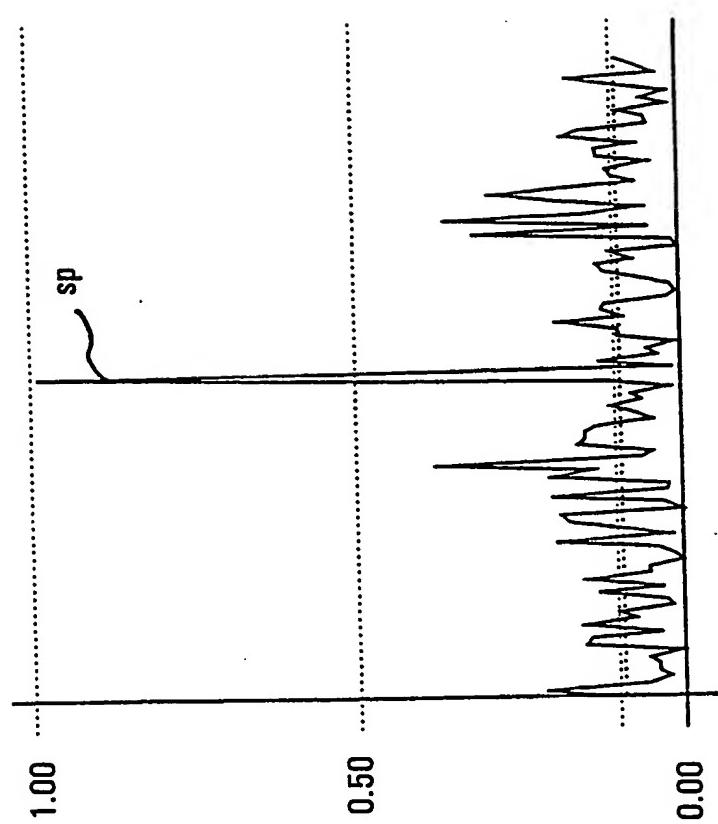
Fig. 7

Fig. 8

Fig. 9

Fig. 10

spt

0.3

0.2

0.1
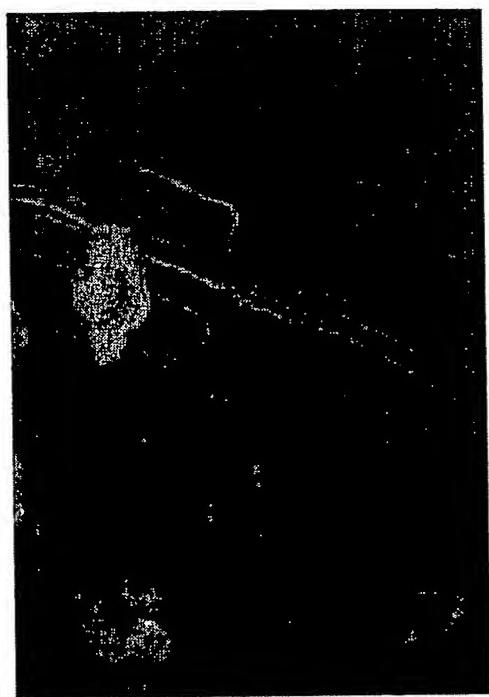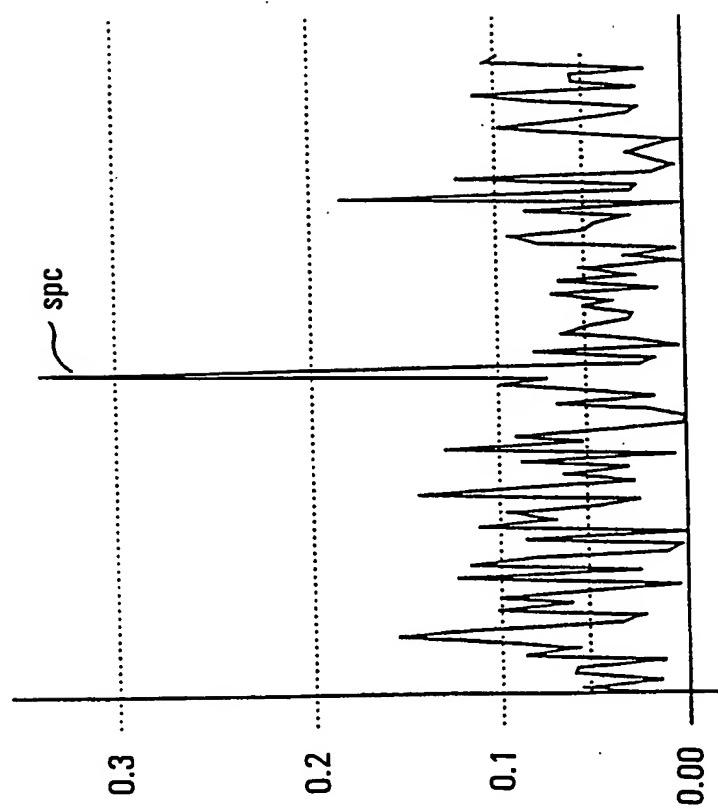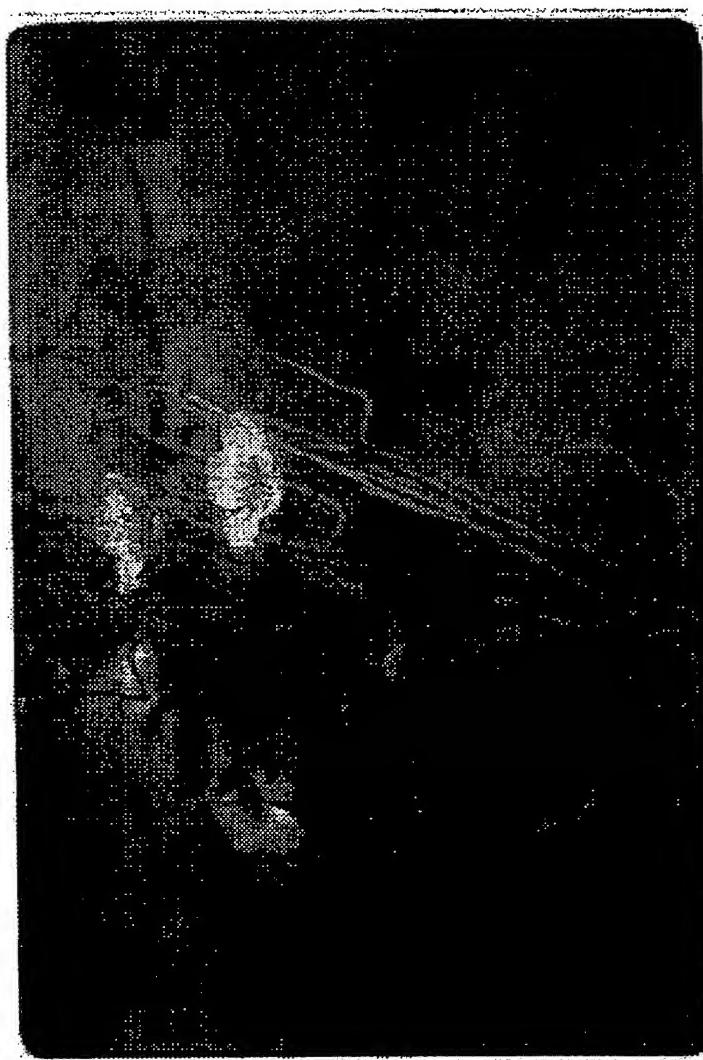
0.00
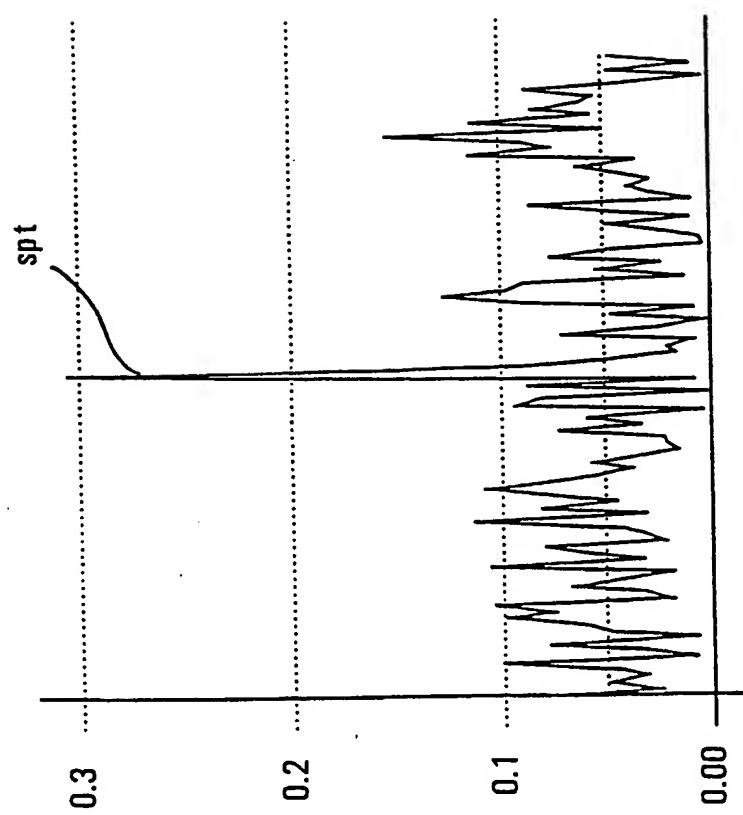
Fig. 11

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6   H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE 1996 IEEE INTERNATIONAL CONFERENCE IN IMAGE PROCESSING, vol. 3, 16 - 19 September 1996, pages 227-230, XP002090178	1-3, 17-19
Y	see the whole document	4-7,20, 21

Y	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996, pages 99-110, XP000604065	4-7,20, 21
A	see the whole document	14-16,24

	-/--	

[X] Further documents are listed in the continuation of box C.   [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 1999	28/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hubeau, R

Form PCT/ISA/210 (second sheet) (July 1992)

2

INTERNATIONAL SEARCH REPORT

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 see column 2, line 18 - column 3, line 25 -----	1-3, 17-19

2

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5499294 A	12-03-1996	NONE	